UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,656	09/18/2003	Carol Ann Egan	ROC920030111US1	8562

30206 7590 11/14/2008

IBM CORPORATION
ROCHESTER IP LAW DEPT. 917
3605 HIGHWAY 52 NORTH
ROCHESTER, MN 55901-7829

EXAMINER	
DAO, THUY CHAN	
ART UNIT	PAPER NUMBER
2192	
MAIL DATE	DELIVERY MODE
11/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/665,656	EGAN ET AL.	
	Examiner	Art Unit	
	Thuy Dao	2192	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34 and 36-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34 and 36-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the amendment filed on August 6, 2008.

2. Claims 1-34 and 36-54 have been examined.

Response to Amendments

3. In the instant amendment, claims 1, 30, and 54 have been amended.

Claim Objections

4. Claim 33 is objected to because of minor informality. Claims 32 and 33 recites identical limitations. In view of claim 4, the phrase in claim 33 is considered to read as --...*comprises a change to the [[hardware]] software configuration*...--.

Appropriate correction is requested.

Response to Arguments

5. Applicants' arguments have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections – 35 USC §103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-34 and 36-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over "SafePatch Version 0.9 Manual", March 1999 (art made of record, hereafter "SafePatch") in view of US Patent No. 7,073,172 to Chamberlain (art made of record, hereafter "Chamberlain").

Claim 1:

SafePatch discloses *a method for providing autonomic, event-driven upgrade maintenance of one or more software modules residing on a computer system, the method comprising:*

detecting a predefined triggering event on the computer system indicative of a potential maintenance issue, the predefined triggering event being triggered by a current operating condition of the computer system (e.g., page 2, section 1.1.2, SafePatch Agent monitors remote system and triggers scheduled updates; page 1, SafePatch Overview; page 43, steps 1-3 and related text)*;*

connecting to an upgrade management server, based upon a set of user defined policies residing on the computer system (e.g., pp. 17-20, SafePatch Server; page 43, steps 3-5 and related text)*;*

creating on the upgrade management server a list of recommended upgrade modules to download to the computer system, the list based upon a set of selection policies (e.g., pp. 9-16, connecting to specified Vendor Server based on policies; pp. 37-38 recommended patches; page 43, steps 4-6 and related text)*;*

downloading a set of recommended upgrade modules from the upgrade management server to the computer system (e.g., pp. 31-33, scheduling/modifying update jobs; page 43, steps 6-7 and related text)*; and*

selectively installing upgrade modules chosen from the set of recommended upgrade modules on downloaded to the computer system (e.g., page 2, section 1.1.1.2, local system administrators may selectively install or not, install in part or whole package).

SafePatch does not explicitly discloses *selectively installing upgrade modules chosen from the set of recommended upgrade modules on downloaded to the computer system, based upon the set of user defined policies residing on the computer system.*

However, in an analogous art, Chamberlain further discloses *selectively installing upgrade modules chosen from the set of recommended upgrade modules on downloaded to the computer system based upon the set of user defined policies*

residing on the computer system (e.g., col.16: 10-23; col.17: 61 – col.18: 12; col.22: 62 – col.23: 17; col.7: 16-39; col.9: 20 – col.10: 14).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to combine Chamberlain's teaching into SafePatch's teaching. One would have been motivated to do so to patch a software implementation on demand as suggested by Chamberlain (e.g., col.3: 6-28; col.11: 2-28).

Claim 2:

SafePatch discloses *the method of claim 1, wherein the method further comprises the step of: notifying a user of the status of the upgrade maintenance operation* (e.g., pp. 1-3 and 17-19).

Claim 3:

SafePatch discloses *the method of claim 1, wherein the predefined triggering event comprises a change to the hardware configuration of the computer system* (e.g., pp. 14-16 and 21-23).

Claim 4:

SafePatch discloses *the method of claim 1, wherein the predefined triggering event comprises a change to the software configuration of the computer system* (e.g., pp. 28-31 and 47-48).

Claim 5:

SafePatch discloses *the method of claim 1, wherein the predefined triggering event comprises exceeding a predefined error threshold on the computer system* (e.g., pp. 36-38).

Claim 6:

SafePatch discloses *the method of claim 1, wherein the predefined triggering event comprises exceeding a predefined performance threshold on the computer system* (e.g., pp. 1-3 and 39-40).

Claim 7:

SafePatch discloses *the method of claim 1, wherein the predefined triggering event comprises exceeding a predefined elapsed time since the last connection to the upgrade management server* (e.g., pp. 14-16 and 39-41).

Claim 8:

SafePatch discloses *the method of claim 1, wherein the steps of connecting to a upgrade management server and selectively installing the list of recommended upgrade modules are controlled by a set of user defined policies* (e.g., pp. 5-7 and 30-33).

Claim 9:

SafePatch discloses *the method of claim 8, wherein the set of user defined policies includes a preferred connection time* (e.g., pp. 12-15 and 47-48).

Claim 10:

SafePatch discloses *the method of claim 8, wherein the set of user defined policies includes the connection resource to be used* (e.g., pp. 21-23 and 32-44).

Claim 11:

SafePatch discloses *the method of claim 8, wherein the set of user defined policies includes the specification of computer system areas/software products to enable automatic application of upgrades* (e.g., pp. 2-6 and 30-33).

Claim 12:

SafePatch discloses *the method of claim 8, wherein the set of user defined policies includes a defined time to connect to the upgrade management server to check for upgrades* (e.g., pp. 17-19 and 44-46).

Claim 13:

SafePatch discloses *the method of claim 8, wherein the set of user defined policies includes a defined elapsed time interval for connecting to the upgrade management server to check for upgrades* (e.g., pp. 2-5 and 39-41).

Claim 14:

SafePatch discloses *the method of claim 8, wherein the set of user defined policies includes a notification list for e-mailing user of information and actions relative to the upgrade management process* (e.g., pp. 14-16 and 28-31).

Claim 15:

SafePatch discloses *the method of claim 8, wherein the set of user defined policies include a list of one or more upgrade management servers to be used for the upgrade management process* (e.g., pp. 21-23 and 42-44).

Claim 16:

SafePatch discloses *the method of claim 1, wherein the one or more computer software modules comprises software applications* (e.g., pp. 2-7).

Claim 17:

SafePatch discloses *the method of claim 1, wherein, the one or more computer software modules comprises operating systems* (e.g., pp. 1-3 and 14-16).

Claim 18:

SafePatch discloses *the method of claim 1, wherein the one or more computer software modules comprises device drivers for installed hardware components* (e.g., pp. 6-9 and 28-31).

Claim 19:

SafePatch discloses *the method of claim 1, wherein the set of selection policies is sent from the computer system to the upgrade management server* (e.g., pp. 31-33).

Claim 20:

SafePatch discloses *the method of claim 19, wherein the set of selection policies includes creating the list of recommended upgrade modules based upon a specific set of upgrades requested by the computer system* (e.g., pp. 37-39).

Claim 21:

SafePatch discloses *the method of claim 19, wherein the set of selection policies includes comparing a revision levels of the one or more software modules residing on the computer system against a revision levels of one or more software modules residing on the upgrade management server* (e.g., pp. 9-14).

Claim 22:

SafePatch discloses *the method of claim 19, wherein the set of selection policies includes creating the list of recommended upgrade modules by identifying modules associated with a hardware change on the computer system* (e.g., pp. 2-6 and 30-33).

Claim 23:

SafePatch discloses *the method of claim 19, wherein the set of selection policies includes creating the list of recommended upgrade modules by identifying software modules associated with a software change on the computer system* (e.g., pp. 14-16 and 42-45).

Claim 24:

SafePatch discloses *the method of claim 19, wherein the set of selection policies includes creating the list of recommended upgrade modules by identifying upgrades specifically associated with an error triggering event on the computer system* (e.g., pp. 17-19 and 26-29).

Claim 25:

SafePatch discloses *the method of claim 19, wherein the set of selection policies includes creating the list of recommended upgrade modules by identifying upgrades specifically associated with a performance triggering event on the computer system* (e.g., pp. 3-7 and 21-23).

Claim 26:

SafePatch discloses *the method of claim 19, wherein the set of selection policies includes creating the list of recommended upgrade modules by analyzing a problem history provided by the computer system* (e.g., pp. 1-4 and 36-39).

Claim 27:

SafePatch discloses *the method of claim 19, wherein the set of selection policies includes creating the list of recommended upgrade modules by identifying compatible revision levels between two or more software modules included within the list of modules* (e.g., pp. 14-17 and 31-34).

Claim 28:

SafePatch discloses *the method of claim 1, wherein the step of downloading the list of recommended upgrade modules from the upgrade management server to the computer system further comprises the step of downloading the upgrade modules themselves from the upgrade management server to the computer system* (e.g., pp. 5-9 and 45-48).

Claim 29:

SafePatch discloses *the method of claim 1, wherein the step of selectively installing upgrade modules chosen from the list of recommended upgrade modules on the computer system further comprises the step of downloading any upgrade modules chosen from the list of recommended upgrade modules from the upgrade management server to the computer system prior to the install* (e.g., pp. 1-4 and 28-32).

Claims 30-34 and 36-53:

Claims 30-34 and 36-53 recite(s) the same limitations as those of claims 1-29, wherein all claimed limitations have been addressed and/or set forth above. Therefore, as the reference teaches all of the limitations of the above claim(s), it also teaches all of the limitations of claims 30-34 and 36-53.

Claim 54:

SafePatch discloses *a method for deploying computing infrastructure, comprising integrating computer-readable code into a computing system, wherein the code in combination with the computing system is capable of providing autonomic, event-driven upgrade maintenance of one or more software modules residing on a computer system, the method comprising the steps of:*

detecting a predefined triggering event on a computer system indicative of a potential maintenance issue, the predefined triggering event being triggered by a current operating condition of the computer system (e.g., page 2, section 1.1.2, SafePatch Agent monitors remote system and triggers scheduled updates; page 1, SafePatch Overview; page 43, steps 1-3 and related text)*;*

connecting to an upgrade management server, based upon a set of user defined policies residing on the computer system (e.g., pp. 17-20, SafePatch Server; page 43, steps 3-5 and related text)*;*

creating on the upgrade management server a list of recommended upgrade modules to download to the computer system, the list based upon a set of

selection policies (e.g., pp. 9-16, connecting to specified Vendor Server based on policies; pp. 37-38 recommended patches; page 43, steps 4-6 and related text);

downloading a set of recommended upgrade modules from the upgrade management server to the computer system (e.g., pp. 31-33, scheduling/modifying update jobs; page 43, steps 6-7 and related text); *and*

selectively installing upgrade modules chosen from the set of recommended upgrade modules on downloaded to the computer system (e.g., page 2, section 1.1.1.2, local system administrators may selectively install or not, install in part or whole package).

SafePatch does not explicitly discloses *selectively installing upgrade modules chosen from the set of recommended upgrade modules on downloaded to the computer system, based upon the set of user defined policies residing on the computer system.*

However, in an analogous art, Chamberlain further discloses *selectively installing upgrade modules chosen from the set of recommended upgrade modules on downloaded to the computer system based upon the set of user defined policies residing on the computer system* (e.g., col.16: 10-23; col.17: 61 – col.18: 12; col.22: 62 – col.23: 17; col.7: 16-39; col.9: 20 – col.10: 14).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to combine Chamberlain's teaching into SafePatch's teaching. One would have been motivated to do so to patch a software implementation on demand as suggested by Chamberlain (e.g., col.3: 6-28; col.11: 2-28).

Conclusion

8. Applicants' amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication should be directed to examiner Thuy Dao (Twee), whose telephone/fax numbers are (571) 272 8570 and (571) 273 8570, respectively. The examiner can normally be reached on every Tuesday, Thursday, and Friday from 6:00AM to 6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Q. Dam, can be reached at (571) 272 3695.

The fax phone number for the organization where this application or proceeding is assigned is (571) 273 8300.

Any inquiry of a general nature of relating to the status of this application or proceeding should be directed to the TC 2100 Group receptionist whose telephone number is (571) 272 2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Thuy Dao/
Examiner, Art Unit 2192

/Tuan Q. Dam/
Supervisory Patent Examiner, Art Unit 2192